PCT / GB00/02531
Sept 00 #2

Europäisches Patentamt | European Patent Office | Office européen des brevets

GB00/02531

Bescheinigung | Certificate | Attestation

4

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

99305219.0

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts:
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE, 11/09/00
LA HAYE, LE

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.: 99305219.0
Demande n°:

Anmeldetag:
Date of filing: 01/07/99
Date de dépôt:

Anmelder:
Applicant(s):
Demandeur(s):
BRITISH TELECOMMUNICATIONS public limited company
London EC1A 7AJ
UNITED KINGDOM

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Data processing apparatus

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
G06F15/80, H04J14/00, G02B6/00

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du dépôt:

Bemerkungen:
Remarks:
Remarques:

Data Processing Apparatus

Description

This invention relates to a data processing apparatus.

Traditional computer architectures systems are well suited to processing data according to predefined algorithms such as by a conventional Von Neumann digital processor. However, such conventional data processing is not generally suited to problems involving analog signals, pattern matching and asynchronous or real-time signals, and also in noisy or chaotic systems or those where the algorithm to be used is unknown and is to be determined by processing of the data.

Neural nets have been proposed for pattern recognition and other purposes but they are not able to adapt rapidly to changes in the system parameters and require extensive training.

The present invention seeks to provide an improved general purpose data processing apparatus which overcomes these difficulties.

According to the present invention there is provided data processing apparatus comprising: a backplane for data signals in a plurality of different formats, a plurality of adaptive filters to receive data signals in respective different formats from the backplane, a plurality of processors to receive data derived from the backplane in said different formats respectively, at least one of the processors being operable to process data from one of the filters and being responsive to the outcome of data filtering performed by at least one other of the filters to adapt the processing performed thereby.

The apparatus according to the invention is not limited to any particular technology, medium or transport mechanism for the signals of different formats, which for example, can be optical, electrical, chemical or any other suitable form.

The use of signals in different formats allows data to be analysed from different perspectives so that a processor operable with signals in a first format may be configured to perform efficient processing on the basis of an analysis of the signals in a second different format.

To this end, a feedback path may be provided to adjust filtering characteristics of at least one of the adaptive filters as a function of the outcome of the processing performed by at least one of the processors.

The feedback may be configured to achieve homeostasis.

At least one of the processors may be operable to carry out processing according to a plurality of different algorithmic processes and to select one of them according to the outcome of the processing performed by another of the processors. Thus, the processing of data in one of the formats can be used to optimise processing of the data in another of the formats so as to provide more efficient algorithmic processing of the data.

In order that the invention may be more fully understood an embodiment of thereof will now be described by way of example with reference to the accompanying drawings, in which:

Figure 1 is a schematic block diagram of an architecture for a data processing apparatus according to the invention;

Figure 2 is a schematic diagram of operation of the architecture shown in Figure 1;

Figure 3 is a schematic illustration of the relationship between an entity and its attributes;

Figure 4 is a schematic diagram of how entities are related through their attributes; and

Figure 5 is a schematic block diagram of a code breaking machine in accordance with the invention.

Referring to Figure 1, the data processing apparatus includes an array of sensors 1 which provide signals in a number of different formats relating to an external

environment in response to inputs I. The sensors 1 produce outputs in different signal formats which are fed into a multi-format communications backplane 2. As explained in more detail hereinafter, the backplane 2 acts as a conduit for signals in different formats, such as optical, electrical, chemical.

A series of connections 3 extend from the backplane 2, to individual adaptive filters 4 which individually recognise some physical property of signals on the backplane 2. For example, one of the filters 4 may be an optical filter configured to recognise a particular optical characteristic of signals from the backplane whereas another one of the filters 4 may be an electrical filter for filtering electrical signals from the backplane. The filters may recognise characteristics such as frequency or some other characteristics such as the signal's chaotic state.

Each of the adaptive filters 4 has an associated processor 5 capable of processing signals in the individual formats handled by the filters. The result of the filtering and processing is fed back on path 6 to the backplane 2 so that the processed signals can be then pass to another filter-processor combination 4, 5 for further processing.

As shown in Figure 1 processor 5a produces an output 6a which passes out of the apparatus. Additionally, an array of transducers/effectors 7 can be provided, responsive to the outputs of the processors 5 to provide an output 6 which can be used to control other processor/filter combinations or communicate with external apparatus.

In operation, inputs I are present in the environment, are detected by the sensor array 1 so as to place signals on the universal backplane 2. The signals may be of any suitable form in different formats, as previously described, and the role of the backplane 2 is to ensure that all of the processor/filter components can receive signals in corresponding appropriate formats from the backplane. The formats may include optical, photonic, liquid or gaseous movement, changes of state and the connections may be achieved in free space or constrained for example in a fibre or tube. Modes of communication may be analog or digital in the backplane 2.

Preferably, the modes of communication in the backplane are inherently multi-modal. For example, an optical fibre can transmit both on many wavelengths and either analog or digital signals. The backplane 2 may perform differential attenuation of signals and may exhibit different temporal characteristics to different signals.

The adaptive filters 4 connected to the backplane 2, select from the signals of different formats those that they can recognise. This will depend on the physical properties and the algorithmic nature of the signal. For example, an optical filter 4 can be set to a particular wavelength, signal threshold and window time, thus acting as a filter element tuned to particular signals. The filter can also act as a buffer by looking only for signals that exhibit a particular short term periodicity. The filter would respond purely to analog signals at the same wavelength and thus some signals from the backplane can strongly stimulate certain filters and weakly or differentially be detected by other ones of the filters.

The filters 4 are adaptive and thus change their filtering properties according to the signals that are acted upon by them. The filtered signals 6 are used to adjust the characteristics of the filters 4 adaptively.

The more that a processor 5 responds to a particular filtered signal, the stronger should be the reinforcement. The filter 4 can be considered as accepting signals inside certain bounds which the overall apparatus can alter. For example, bounding of the filtered signals in terms of wavelength, threshold and window duration can be carried out. The effect of the feedback to the adaptive filters 4 is either to increase or decrease bounding of the filter. The exact mechanism will depend on the processor 5 and the filter 4. The goal is to reinforce desirable behaviours. The bounding could even initially increase response strength and then decrease so that the filter 4 self-tunes to an optical response level.

The processors 5 are configured to receive filtered inputs from the filters 4 and to carry out an algorithmic process to provide an output. The processors 5 may take many different forms. They may comprise conventional digital processors or can

operate according to an analog computation, involve interaction with humans, be a wet chemical, electronic or other action. The processors 5 may include individual memories to store precise, imprecise or temporally failing data. Unlike a conventional Von Neumann processor, there may not be a requirement for a dedicated conventional memory store, but instead, memory elements may be distributed throughout the processor architecture, for example in the backplane 2 or the filters 4.

Figure 2 provides an insight into how the architecture will operate to produce an effective output 6, having been stimulated at its input 1a.

In Figure 2, a number of vectors are shown, as follow:

P Vector that represents a problem space
K Vector that represents a knowledge space
S Vector that represents a solution space
B Vector that represents a bounding function
erf I Vector that represents an error function

The apparatus in basic terms produces a solution, or a manipulation of an effector, by operating a transform from the problem space P which acts with the knowledge space K to create a solution or a number of solutions in the solution space S. The bounding vector or B is used to bound the solution.

The error function erf I is used to stimulate the machine randomly and/or synchronously in order to prevent it from falsely locking into a limited solution space. Although in Figure 2, the process is presented in two dimensions for each of explanation, it will be understood that the architecture of Figure 1 has the capability to operate in N dimensions.

Each element of the P, K, and S vectors consist of a single entity which has a number of attributes associated with it, as indicated in Figure 3. The machine builds its knowledge space K by creating entities and associate attributes with each entity. The machine links the attributes, which are not permanent in time, and the

links are continually reviewed and reinforced as appropriate. If the links are used often, then they are reinforced because it indicates a strong association between the entity and the attribute. If the link is used less often, it is weak and is removed relatively quickly.

Figure 4 illustrates schematically how entities are related through their attributes. Figure 4 illustrates entity groups E1, E2, E3, and E4 and E5.

Knowledge K is associated with an entity E, where:

E1 represents a dog
E2 represents a cat
E3 represents a mink
E4 represents a car
E5 represents a locomotive

An attribute that could link groups E1, E2 and E3 is fur. An attribute that could link group E4 and E5 is steel.

The same rules apply to the linking of attributes as to the linking of an entity to an attribute.

Example

The architecture shown in Figure 1 together with the functionality described with reference to Figures 2 and 3 can be used with advantage to provide a code breaker and an example of code breaker machine architecture is shown in Figure 5.

There is an inherent problem with employing conventional digital computers to crack encrypted code. The conventional method is to use a plurality of code cracking algorithms which are coded into the computer and then the computer number crunches until it achieves a solution, if possible. A problem with this method is that there are a large number of data combinations that the computer needs to investigate and so if it starts in the right part of the checking sequence, it

could reach a solution relatively quickly whereas if it starts spuriously in the wrong part of the solution space, the solution may take much longer to achieve.

In accordance with the invention, this inefficiency is improved by using additional processing techniques on the signals in different formats in order to provide the computer with an indication of where to start looking for a solution. This minimises the random nature of how long the digital computer takes to break code. Conventional code breaking algorithms are run on processor/filter combinations 4a/5a, and additional processing is carried out by processors and filters 4b, 5b and 4c, 5c.

An electrical signal I, which may comprise a signature or password created by the multiplication of two prime numbers, is fed as an input to the element 1, which produces signals in two different formats. In this example, the element 1 comprises an electro-optical modulator, e.g. a laser which receives the input signals I as electrical signals and converts them into corresponding optical pulses. The backplane 2 comprises an electrical line 2a e.g. a coaxial cable which acts as a conduit for the input digital electrical signals I. The modulator 1 produces corresponding digital optical signals that are fed to a second conduit 2b in the form of an optical fibre.

A processor 5b, in the form of a spectral analyser is responsive to the characteristics of the electrical signals in the backplane 2. The analyser 5b is capable of making measurements e.g. from 0-10 GHz with integral filtering functionality thereby providing an inherent adaptive filter 4b. When the element 5b initially senses the electrical coded signal I on the conduit 2a, its filter 4b is set to maximum bandwidth namely 0 - 10GHx. The analyser then takes measurements in relation to the signal frequency, amplitude and power of the signals and upon analysing the measurements, modifies the bandwidth of the filter in order to band limit the spectrum of measurement. This modification of the filter from its maximum bandwidth to a band limited value, constitutes learning and homeostasis, as the filtering is adapted in response to an analysis of the incoming electrical signal. As long as there is no or little change in the input coded signal from conduit 2a, the filtering will stay in a relatively constant state, but will change in response to changes in the input signal

characteristics. Additionally, data from the filter 4a/processor 5a can provide feedback through the electrical wiring to the filter 4b to allow its characteristics to be adaptively changed. Examples of suitable spectrum analysers are HP4395-500MHz, HP4936-1.8GHz, HP8757-40GHz.

The optical signals produced on the conduit 2b are detected by a processor/filter arrangement 5c, 4c capable of performing an optical Fourier transform. The device may comprise a dispersive optical element which has an array of optical receivers which form the output of the filter 4c. When the optical signal is presented to the Fourier transformer, it produces a corresponding pattern in the focal plane of the device which is detected and hence characterised by the optical receiver array 4c. When the coded signal applied to the transformer is modified, the output from the array is consequently changed. The element 4c/5c includes a memory and a simple processing capability to enable particular output patterns for the sensor array 4c to be stored and correlated with particular forms of input code from the optical fibre 2b.

The output from the sensor array 4 comprises an electrical signal 3a which is applied to the electrical conduit 2a.

A conventional digital processor 5a such as a Pentium ™ or similar digital processor with an associated input filter functionality 4a is coupled to the electrical conduit 2a. The filter functionality may provided by software running on the processor or by the provision of an individual processor dedicated to the filtering function. The processor 5a includes a conventional memory and holds a number of different algorithms/programs that can be used to decipher the encrypted code on the conduit 2a. In use, the processor 5a uses the algorithms to attempt to break the code. The processor 5a tries all of the individual programs in a sequence. As an example one of the algorithms may configured as described in "Breaking DES", Paul C Kocher, published by RASA Laboratories in CryptoBytes, the Technical newsletter of RSA Laboratories, a Division of RSA Data Security Inc, Volume 4, Number 2, Winter 1999. Another algorithm may be as described in "Attacking Elliptic Curve Cryptosystems

Using Parallel Pollard rho Method' by Adrian E Escott, Alexander P L Selkirk & Dimitrios Tsapakidis, in the same publication.

The incoming data from the conduit 2a is provided with an identification label by the processor 5a. This label is communicated through the backplane 7 to the other processors 5b, 5c where it is stored and associated with the filtered outputs produced by the filters 4b and 4c. This common label is used to associate the coded signal with the most efficient method employed to crack the code.

Once the processor 5a has identified a solution for the encrypted data, it carries out a safety check on the solution and possibly refers the solution to a human operator for final checking, on output 6a. Then, assuming that the solution satisfies the criteria, the previously mentioned code label associated with the encrypted signals is associated with the solution itself. This association performs two functions. The first is to allow the machine to learn, so that each time a code is entered into the machine and has already been labelled, then the machine, from its previous experience knows what algorithms are suited to solving it. Thus, the processor 5ais directed to perform algorithmic processing in a particular sub-set of its possible range of possibilities rather than use the complete set of algorithms that are available, thereby speeding up the process.

The processor 5a also carries out a checking of the solution obtained from the code breaking algorithms in order to determine whether a solution has been found or whether further attempts to break the code are required using different algorithms.

An example will now be considered in which the machine shown in Figure 5 is used to crack a signature or password that was created by multiplying two prime numbers. The machine thus is required to determine the two prime numbers from encrypted data comprising the multiplication thereof on input I.

The problem of trying to crack the code with a conventional digital processor requires the processor to number crunch through each and every combination of prime numbers until an appropriate corresponding encrypted code is produced, so

as to determine the solution. The speed at which the code will be cracked, is indeterminate as it is a function of where in the number of possibilities available, the algorithm started to check the various combinations.

When the machine of Figure 5 is first switched on, it has no knowledge of the characteristics of the encrypted signal applied to input I or which algorithm should be employed in processor 5a to crack the code. When the first encoded signal is presented to the machine, all of the processors 5a, b, c operate on the signal. As a first operation, the coded signal is characterised by each of the processors and associated with the aforementioned label generated by processor 5a. Once characterised, the machine is able to identify the form of the code, in this case the multiplication of two prime numbers. This may need intervention by a human operator. Having identified the make up of the code, the processor 5a will employ one of a number of number-crunching algorithms to crack the code. The first time that the machine carries out this process, it does not know where to start the algorithm and therefore the process may take along time. Once having cracked the code, the processor 5a will associate the code label with the corresponding solution so as to associate a particular part of the solution space provided by the algorithm with the solution. Each time a new code is presented to the machine, it will start to build a knowledge of the corresponding labels associated with the incoming data which relate to the code characteristics so as to learn where to look for a solution rather than try all possible solutions.

When the machine is initially turned on, instead of just applying a coded signal that requires decoding, it will be possible to take a range of codes which the user has created and therefore for which the solution is known, and use these to teach the machine.

Claims

Data processing apparatus comprising:

a backplane for data signals in a plurality of different formats,

a plurality of adaptive filters to receive data signals in respective different formats from the backplane, and

a plurality of processors to receive data derived from the backplane in said different formats respectively, at least one of the processors being operable to process data from one of the filters and being responsive to the outcome of data filtering performed by at least one other of the filters to adapt the processing performed thereby.

2. Apparatus according to claim 1 including a feedback path to adjust filtering characteristics of at least one of the adaptive filters as a function of the outcome of the processing performed by at least one of the processors.

3. Apparatus according to claim 1 or 2 wherein at least one of the processors is operable to carry out processing according to a plurality of different algorithms and to select at least one of them according to the outcome of processing performed by another of the processors.

4. Apparatus according to any preceding claim wherein the backplane includes an first conduit for signals in a first format and a second conduit for signals in a second format.

5. Apparatus according to claim 4 wherein the filters include a first filter to filter the signals in the first conduit and a second filter to filter the signals in the second conduit.

6. Apparatus according to claim 4 or 5 wherein the processors include a first processor to process signals derived from the first conduit and a second processor to process signals derived from the second conduit.

7. Apparatus according to claim 4, 5 or 6 including an input to receive input signals to be processed and to supply the signals to the first and second conduits in the first and second formats.

8. Apparatus according to any one of claims 4 to 7 wherein the first and second conduits are configured to convey optical and electrical signals respectively.

9. A data processing method for data manifested as signals in a plurality of different formats, comprising:
adaptively filtering the data signals in the different formats respectively, and individually processing the signals in said different formats respectively, such as to process data in one of the formats that has been subject to the adaptive filtering, adaptively in response to the outcome of data filtering performed on data in at least one other of the formats.

10. A method according to claim 9 including adjusting the filtering of data in one of the formats as a function of the outcome of the processing performed in another of the formats.

11. A method according to claim 9 or 10 including selecting the processing for data in one of the formats from a plurality of different algorithms according to the outcome of processing performed on the data in another of the formats.

Abstract

Data processing apparatus

A data processor operates on data in different formats to improve computational efficiency in a complex system. The processor comprises a backplane (2) for data signals in different formats such as electrical and optical formats, adaptive filters (4) that receive data signals in the different formats from the backplane, and processors (5) to receive data derived from the backplane in the different formats, at least one of the processors being operable to process data from one of the filters and being responsive to the outcome of data filtering performed by at least one other of the filters to adapt the processing that is carried out. A code-breaking process is given as an example.

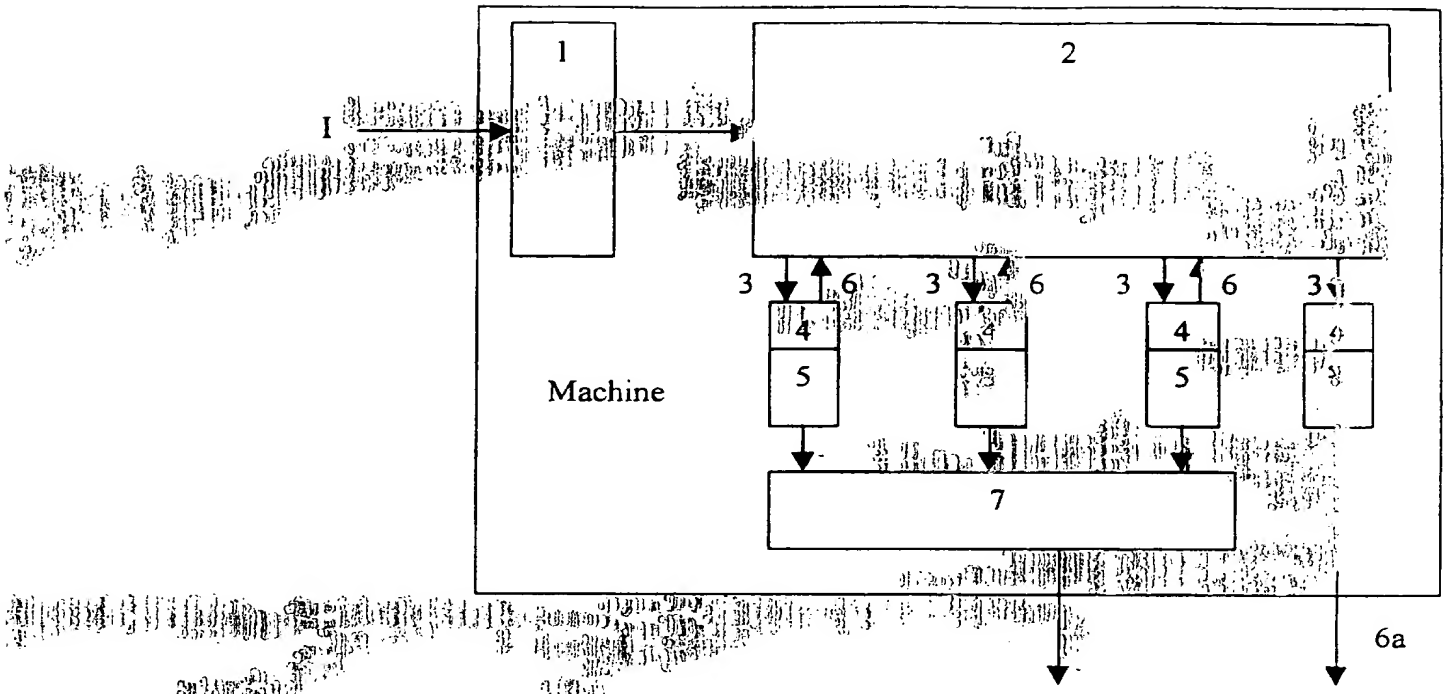

Fig.

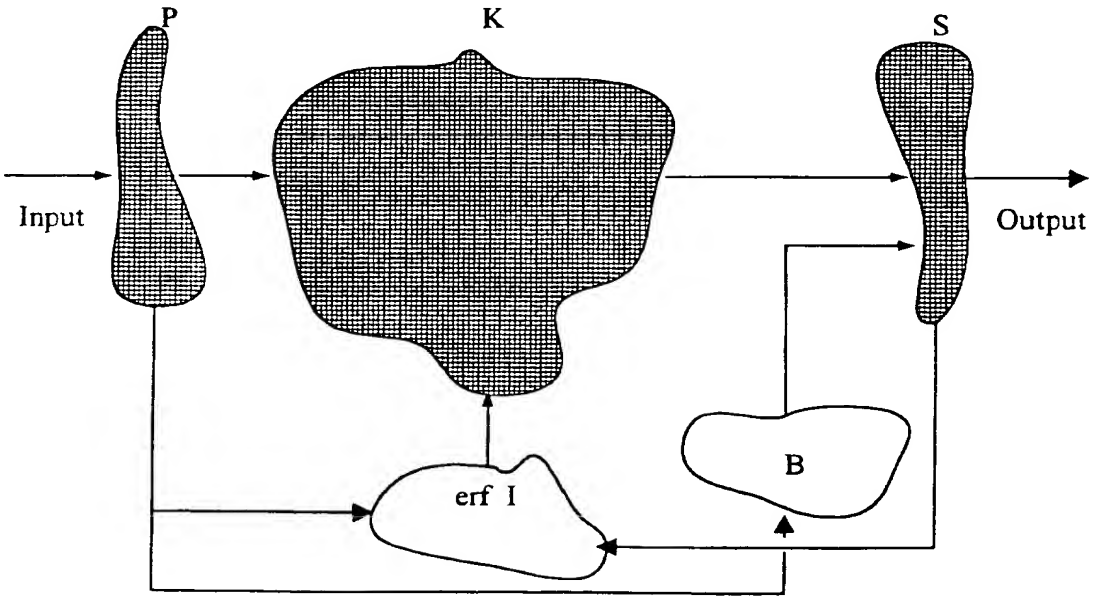

Fig. 2

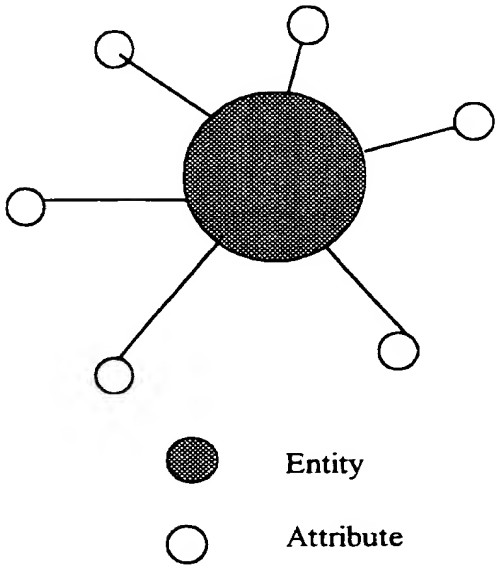

Fig. 3

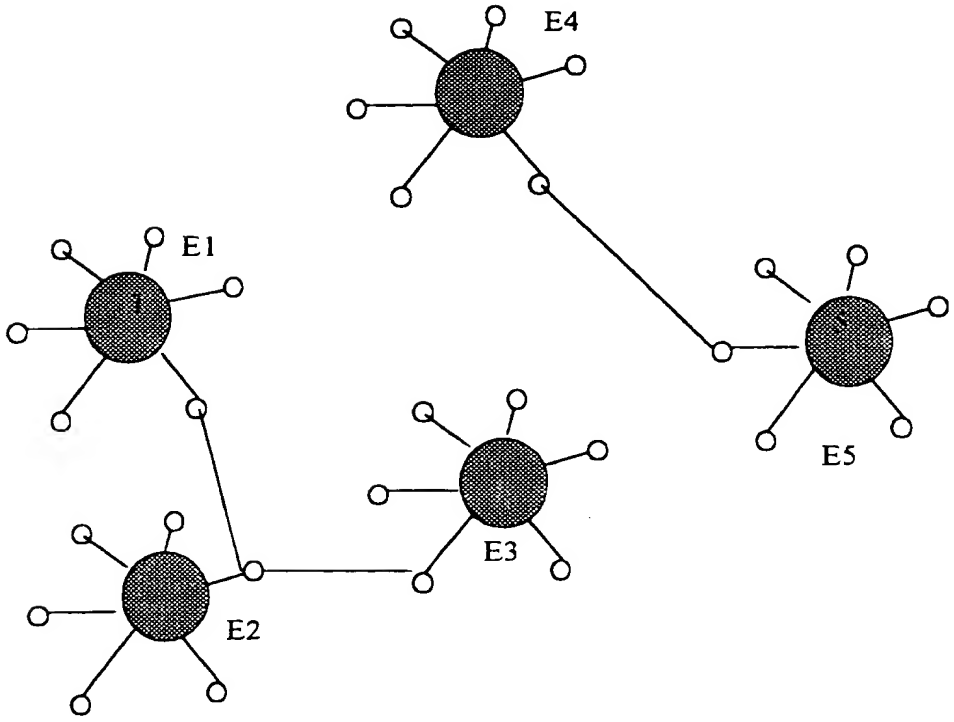

Fig. 4

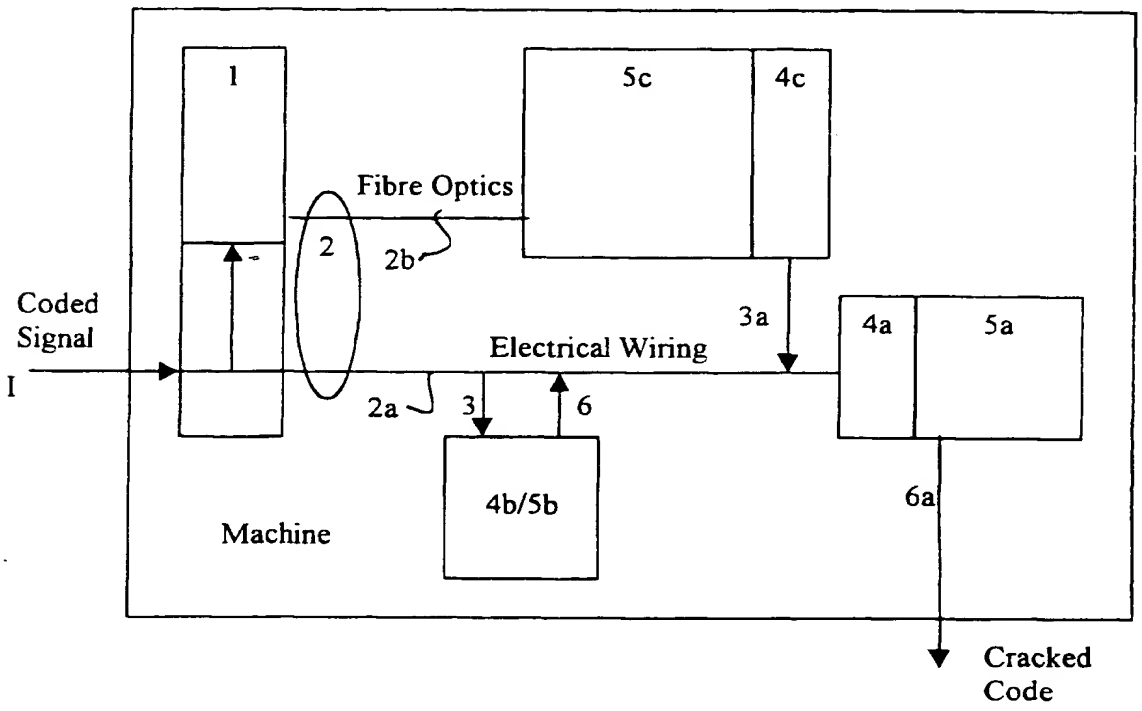
1
5c
4c
Fibre Optics
2
2b
Coded
Signal
I
3a
4a
5a
Electrical Wiring
2a
3
6
4b/5b
6a
Machine
Cracked
Code

Fig. 5